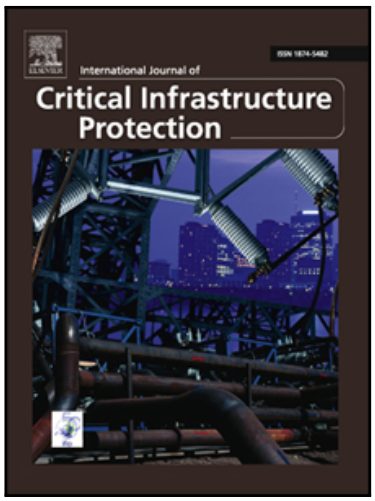
DOI:
10.1016/j.ijcip.2018.12.001

Document Version
Peer reviewed version



The Insider Threat: Behavioral indicators and factors influencing likelihood of intervention

Alison J C Bell , Professor M. Brooke Rogers , Dr Julia M Pearce

PII: S1874-5482(18)30098-2
DOI: https://doi.org/10.1016/j.ijcip.2018.12.001
Reference: IJCIP 284

To appear in: *International Journal of Critical Infrastructure Protection*

Please cite this article as: Alison J C Bell , Professor M. Brooke Rogers , Dr Julia M Pearce , The Insider Threat: Behavioral indicators and factors influencing likelihood of intervention, *International Journal of Critical Infrastructure Protection* (2018), doi: https://doi.org/10.1016/j.ijcip.2018.12.001

Title page

Title: The Insider Threat: Behavioral indicators and factors influencing likelihood of intervention

Authors:

Alison J C Bell [a1]

[a]University of Portsmouth, Winston Churchill Avenue, Portsmouth, Hampshire, PO1 2UP

Professor M. Brooke Rogers[b]

[b]King's College London, Strand Campus, King's College London, London

brooke.rogers@kcl.ac.uk

Dr Julia M Pearce[b]

[b]King's College London, Strand Campus, King's College London, London

julia.pearce@kcl.ac.uk

Corresponding Author: alison.bell.1@kcl.ac.uk

[1] Present address: King's College London, Strand Campus, London, WC2R 2LS

Abstract

The insider threat is a significant security concern for Critical National Infrastructure (CNI) organizations. A successful insider act in one of the CNI sectors has potential to damage assets and interrupt the critical services that society depends upon. Existing research suggests that behavioral indicators are often evident prior to an act taking place, but that reporting of such behaviors does not usually happen. The aim of this study was to identify factors that influence employees' intention to intervene when observing behavioral changes associated with insider acts. An online survey with employees within a large Critical National Infrastructure (CNI) energy sector organization (N=55) explored factors including behavioral change type, relationship to the actor, employment status of the actor and actor motivations. Results supported existing research regarding reluctance to report behavioral indicators of attitude change, but also demonstrated that situations with sufficient evidence are more likely to be reported. Factors which inhibited intervention likelihood were relative seniority and perceived motivations of the actor, confidence of confidentiality and clarity of reporting processes. Primary barriers to intervention related to the observer's perceived ability to correctly interpret behavioral indicators and awareness of how to respond. Organizations need to provide training regarding behavioral indictors of insider threats, clear, confidential reporting processes, and a culture where respectful challenge is encouraged.

Key words: insider threat; bystander intervention; counterproductive workplace behavior; behavioral indicators; reporting

Manuscript

The Insider Threat: Behavioral indicators and factors influencing likelihood of intervention

Abstract

The insider threat is a significant security concern for Critical National Infrastructure (CNI) organizations. A successful insider act in one of the CNI sectors has potential to damage assets and interrupt the critical services that society depends upon. Existing research suggests that behavioral indicators are often evident prior to an act taking place, but that reporting of such behaviors does not usually happen. The aim of this study was to identify factors that influence employees' intention to intervene when observing behavioral changes associated with insider acts. An online survey with employees within a large Critical National Infrastructure (CNI) energy sector organization (N=55) explored factors including behavioral change type, relationship to the actor, employment status of the actor and actor motivations. Results supported existing research regarding reluctance to report behavioral indicators of attitude change, but also demonstrated that situations with sufficient evidence are more likely to be reported. Factors which inhibited intervention likelihood were relative seniority and perceived motivations of the actor, confidence of confidentiality and clarity of reporting processes. Primary barriers to intervention related to the observer's perceived ability to correctly interpret behavioral indicators and awareness of how to respond. Organizations need to provide training regarding behavioral indictors of insider threats, clear, confidential reporting processes, and a culture where respectful challenge is encouraged.

Key words: insider threat; bystander intervention; counterproductive workplace behavior; behavioral indicators; reporting

1.0 Introduction

Critical National Infrastructure (CNI) organizations face many different types of security threats, such as cyber-attacks [1, 2] and physical security breaches which threaten critical networks and key assets [3, 4]. In addition to threats from actors outside the organization, CNI organizations also need to give priority to the insider threat. This is considered to be one of the most important security concerns for organizations and government agencies due to the potential for insider acts to disrupt services and cause physical and reputational damage [5-8]. The insider threat is particularly significant for CNI organizations, where the most damaging insider act has potential to jeopardize ability to deliver essential services and cause disruption to daily life for the general public [9].

The purpose of this study was to determine whether changes in behavior which may be associated with insider acts, would be identified and acted upon by employees of a CNI organization. The insider act can take a number of different forms, such as fraud, terrorism, sabotage, theft of assets, theft of data or intellectual property and espionage [5, 10-12]. High profile instances reported in the media demonstrate the diverse range of insider acts, the potential harm that the insider can cause, and the potential damage that can occur in respect to customers and reputation. Examples of insider acts that have impacted CNI organizations include, but are not limited to: the British Airways software engineer (Rajib Karim) who was passing information to a terrorist organization [13]; Jessica Harper who committed fraud at Lloyds bank [14]; Roger Duronio who sabotaged computer servers at UBS Paine Webber [15], and Waheed Mahmood who considered using his inside knowledge and access to the energy sector to facilitate damage to the gas network as part of a bomb plot linked to Al-Qaeda [16]. Currently, the continuing evolution of and growing reliance upon information technology increases the risk of insiders using this as a mechanism to conduct attacks. As a result, the potential damage that an insider could do is increasing [11].

There are many definitions of the insider threat. One study identified forty-two variations [17]**,** underscoring the difficulty of arriving at an accepted definition [18, 19]. For example, issues of scope fuels debates about whether the term 'insider' refers only to employees or contractors or whether it should also include outsiders who are able to obtain information by coercion or hacking into a company network [5, 6, 18, 20]. Additionally, four of the definitions identified by Mundie et al [17], refer to the ex-employee as a potential insider which creates a complicated 'insider/outsider' category. This can occur, for example, if the exit procedure which removes remote access has not been rigorous or timely enough hence allowing a mechanism for the disgruntled leaver to take their revenge [5]. For this study we used the definition by Cappelli et al [21], which states that the insider is "a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems" [21]. Although this definition focuses on acts associated with information technology, it captures the different types of employee who could act as an insider which is one of the factors that is explored in this study in relation to likelihood of reporting behaviors of concern.

When the insider act materializes, it can have a significant impact on organizations in terms of reputation, share price and ability to continue operating [22]. There are also potential impacts on the other employees in the workforce and the safety, wellbeing and security of the general public. Within the CNI context, the insider act can cause physical damage to production of goods or ability to maintain critical services and there may also be a resulting impact further down the supply chain, as the target organization may not be the only victim [9, 11]. For example, if a CNI organization in the energy sector suffers from an insider act committed by an individual in a critical role which means that electricity supplies are lost as a

result; this might affect transport infrastructure which depends on power to operate, or on other businesses in the area which may have to send staff home. Due to the extent of the damage that the insider act can cause, CNI organizations will usually seek to put a number of controls in place to try to help detect, deter and prevent the insider threat. This might include awareness campaigns designed to help employees understand the insider threat and how it can occur, and pre-employment screening (sometimes referred to as background checking).

Pre-employment screening usually includes checks such as the individual's credit history, criminal record, and employment history, and can be a powerful deterrent against deliberate infiltration (where the individual joins an organization with a predefined purpose to commit the insider act). However, it only provides a snapshot at a single point in time [23]. This is important, as although the threat of deliberate infiltration cannot be ruled out, there is evidence to suggest that an insider act is more likely to be committed by an individual who has been with the company for a while, rather than someone who joins with intent from the outset [11, 24, 25].

Specifically, research conducted by the Centre for the Protection of National Infrastructure (CPNI) in the UK found that 76% of the insider acts they examined were carried out by individuals who did not join the CNI organization with intent to commit the insider act, with the remaining 24% either being exploited by outside parties, or joining with intent [24]. Negative life events and personal circumstances, as well as events within the workplace can occur post pre-employment screening and can lead to vulnerability to the insider act [8, 23, 26]. Furthermore, even if screening is repeated during the employment lifecycle, typical checks are unlikely to determine changes in attitude, allegiance to the organization or whether employees are disgruntled. Therefore, pre-employment screening cannot be relied upon as the sole control within CNI organizations to mitigate the insider act [8, 10, 24]. A further dimension to the insider threat issue is when organizations make attempts to strengthen

security from external threats without consideration of how this impacts their employees. This can have a significant impact on the employee in terms of increased stress and lengthening the time it takes them to complete everyday tasks, and might inadvertently contribute to the insider threat if the employee attempts to bypass security or becomes more vulnerable to social engineering as a result [27, 28].

1.1 Behavioral indicators

In considering what other mechanisms might be used to detect the insider threat to Critical National Infrastructure (CNI) organizations, there is strong evidence to suggest that insiders are likely to exhibit noticeable changes in their everyday behavior and display some type of concern or indicator leading up to, and during the act being committed [12, 23, 24, 29-33]. Behavior in the workplace might traditionally be considered to be solely an issue for management or HR to deal with; however evidence suggests that there could be scope for employees and team members to intervene and potentially disrupt an insider act. For example, behaviors of concern were observed by management or team workers in 97% of the 49 sabotage incidents examined by Keeney et al [34]. Importantly, multiple studies show that after the insider act happened and the investigation is conducted, colleagues or those who knew the person also indicated that they had noticed behavioral change or indicators prior to or during the attack, irrespective of the type of insider event which took place [11, 24, 26, 32, 34-36]. Additionally, Wood and Marshall-Mies [37] report that there have been espionage cases where behavior and activity has been reported by the person's colleagues leading to the capture of spies, demonstrating that it is possible both to identify behaviors and effectively intervene. This latter example is relevant to CNI organizations as illustrated by the case of Ian Parr who worked in the UK defense sector and attempted to sell classified information to a Russian agent [38].

Behavioral changes can take the form of overt physical actions with evidence, events or incidents which may be reported to Human Resources (HR), or sustained changes in normal behavior or attitudes which may become noticeable to fellow team members. In some cases, the insider may become vocal about their intentions, even to the extent of bragging or making threats about what they plan to do [23, 34, 35]. According to media reports, Chelsea Manning (the US army intelligence analyst who leaked sensitive information to the WikiLeaks website) had allegedly boasted in an on-line networking forum about the actions she had taken [39]. Behavioral changes may also be reflected in the language an insider might use within email correspondence [33].

Furthermore, insiders may be observed carrying out visible actions that are unusual or concerning, such as copying or removing large volumes of data or information, or trying to obtain records that they do not need to carry out their role [24, 34, 37, 40]. Complaining about, or deliberately breaking or ignoring rules that the organization has in place and misusing physical access is also prevalent in many cases [22-24, 34]. These behaviors are generally referred to as anomalous or Counterproductive Workplace Behaviors (CWBs) [41]. Other CWBs related to insider acts include regularly being late, lying, demonstrating bad performance and causing trouble with other employees [22, 34]. Additional observable changes include regular repeat instances where the individual comes into the office out of hours or changes in wealth [10]. The latter is perhaps unsurprisingly a common indicator for fraud cases, whether this is sudden overt signs of excessive wealth or a struggle with debt.

Behavioral indicators of changes in attitudes to work and how the individual feels about the organization are potentially less easy to detect, interpret and successfully act upon, as they are often less evidential and arguably more subjective [22, 35]. A significant and sustained change in behavior or attitude such as an employee who is usually reserved becoming more vocal, or someone who is normally outgoing becoming distanced [42] are examples of

behavioral changes which could be a concern. Although these changes may be observed, they are not necessarily reported. Reporting is less likely if a fellow employee expresses their unhappiness about their work, without displaying any other indicator. It is likely that verbal expression of this nature would fall under the reasonable threshold of seriousness on its own to warrant investigation or disciplinary action and in some organizations might even be considered to be the norm. Furthermore, some indicators might be held separately by a number of different departments within the organization and this can inhibit earlier detection of potential insider risk. For example, Security may hold information about unusual patterns of access to buildings and HR may hold details of 'red flags' or performance issues, as well as information relating to potential employment grievances [7, 10]. Employee information relating to potential grievances associated with for example, organizational restructuring, job insecurity and unsuccessful job applications can be useful as it tends to be fact based or at least considered significant enough to be reported. However, HR will not necessarily be aware of how an employee has responded to being rejected for a new post or whether there are other factors in the individual's working or home life that might cause additional vulnerabilities. They may also be unaware whether these potential flags have manifested in behavioral change within the everyday working environment.

Similarly, the observer who sees the change in behavior may not be aware of the information that HR holds or realize the potential security implications of these changes. For example, Wood & Marshall-Mies [37] found that although a formal obligation exists for US Department of Defense (DoD) to report changes in behavior, this was not being done partly due to lack of awareness of what 'concerning' behaviors meant. Additionally, the observer was not always clear that the behavior was unambiguously a security concern which served to further inhibit reporting [37].

2.0 Theory

The survey underpinning this study was informed by a number of theoretical trends. For example, factors that influence the decision to report can be understood by referring to bystander intervention theory that was initially developed by Latané and Darley [43] following a series of experiments designed to test the 'bystander effect', which occurs when the presence of others discourages onlookers from intervening in an emergency situation. This theory helps explain the behavior of bystanders and their willingness to respond in an emergency by outlining the process of intervention and identifying factors that may inhibit a bystander from intervening. The intervention process is described in several stages, which are to notice; interpret what has been seen; take responsibility for action; decide how to intervene and finally to put the intervention into action [43]. This is a well-established model that has been demonstrated in a variety of different contexts, such as crime [43-48], bullying and harassment [49-52], and countering violent extremism [53]. This framework has also been applied to insider acts, where diffusion of responsibility was found to impact employee challenge of counterproductive work behaviors [54].

Bystander intervention theory identifies a number of factors which may help understand reporting of behaviors associated with insider acts in the workplace. The observer first has to notice the changed behavior, which is more difficult in a busy environment [43]. In the workplace where there are numerous distractions it might not always be possible to observe changes in behavior of colleagues, particularly where these are subtle or ambiguous. We therefore hypothesise that in a CNI organisational context observers would be more likely to report in the scenarios where behavior change was more noticeable. This was tested in the survey by including two scenarios which include behavioral change only, and two scenarios where behavior change was accompanied by evidence that would make this change more noticeable.

Secondly, the observer needs to interpret the behavior as something which should be reported. In the earlier bystander studies it was found that some observers would develop other explanations to account for the behaviors that they have seen, which allowed them to conclude that there was no requirement to intervene [43, 55]. We suggest that this is likely to be a particular issue in the context of behavioral indicators for insider acts, given the inherent ambiguity of interpreting changed behavior in the workplace which could be due to a number of reasons that may not be associated with an insider act. For example, changes in performance might be indicative of issues outside of the work environment such as bereavement or family problems, or health issues. We hypothesise that uncertainty about what has been observed may inhibit intervention, therefore the perceived motivation of the actor and the perceived severity or harm of the behavior was tested within the survey.

An additional factor which may contribute towards uncertainty is competence. The observer may not feel confident in their own ability to determine whether behavior should be reported, particularly if they are unsure about what they have observed and believe that they could be mistaken, therefore we hypothesise that within CNI organisations, the observers perceived lack of competence may inhibit reporting. In considering whether to intervene or not, the observer of insider related behavior may take their perception of the organization's response into account, and if the observer perceives that they will have support from the organization when bringing their concerns forward this might help them to feel more confident. Likewise, if an observer is frightened of the personal consequences which may occur as a result, this can negatively impact the likelihood of intervention [51]. If the organization does not maintain confidentiality for the reporter, this might lead to reprisals particularly if the observer is mistaken. All of these factors will be tested in the survey.

Assuming that the behaviors have been noticed and interpreted as potentially problematic, the observer still has to determine whether they are responsible for intervention and how to

intervene [43]. Intervention can take a number of potential different routes for a CNI employee who has observed behavioral change. They might choose to offer direct help, referred to as 'direct intervention' [43] such as talking to the person themselves to try and establish what is wrong. Alternatively they may ask for help from someone else who they feel is more able to assist, referred to as 'detour interventions' [43]. This might consist of reporting the behavior to a line manager, security or via a helpline. Given that the behavioral indicators are often ambiguous in nature and may gradually develop over time [46], another potential option the observer may take is to wait and observe what else happens. We hypothesised that having an awareness of the intervention and reporting mechanisms which are available and the existence of a clear reporting process, are factors which may increase reporting likelihood.

Finally, bystander intervention theory also highlights the importance of the relationship between the observers and also between the observer and the victim. In studies where the observer had a relationship with the victim, intervention was found to be more likely because the intervention is designed to help the victim and therefore the outcome from the intervention should be positive [49-51, 56, 57]. In situations where this relationship does not exist, the bystander can expect to have limited requirement for continued interaction post intervention [43, 58]. This can make intervention easier because there is no existing relationship and there is less at stake from a personal perspective [53]. However, in the insider act context, such interactions within the workplace may be with longstanding colleagues where there is an existing relationship or with those who are new to the organization where there is less familiarity, and other additional dynamics such as whether the actor is more senior to the observer. We therefore hypothesized that the relationship with the actor would influence the observer, in that intervention would be less likely where the

actor is more senior and where a relationship already exists, but more likely where the actor is not known to the observer.

In conclusion, this work set out to explore the following:

1. Whether reporting might be more likely in the scenarios where behavior change was more noticeable;
2. If uncertainty about what has been observed would inhibit intervention;
3. Whether the observers perceived lack of competence would inhibit reporting;
4. Whether the reporting likelihood might increase if there is a clear reporting process and the observer has an awareness of the intervention and reporting mechanisms which are available;
5. If an existing relationship with the actor would influence intervention, and whether factors such as seniority of the actor would inhibit reporting likelihood.

3.0 Method

The study focused on one large Critical National Infrastructure (CNI) organization in the energy sector. This provides an important context for exploring insider threats to CNI organizations, because other CNI sectors, such as transport and banking are dependent on the provision of power to operate. A successful insider act in a large energy organization could therefore have a significant impact on the provision of key services. In a worst case scenario, failure to provide these services could impact the safety and wellbeing of the general public, as well as cause longer term economic damage [11].

3.1 Design

In this study we used an online survey to identify which types of behavioral indicators would be acted upon or reported by employees of a large CNI organization. A survey was

employed to allow access to a broad range of departments and a cross section of grades (including staff level and managers) to maximize the variety of respondents within the organization. The survey design used four scenarios: two of which described behavioral indicators of attitude change, whilst the other two also involved more overt behavioral changes. Referred to as 'Behavior Change' scenarios, the indicators in the first two scenarios were shifts from normal behavior, where an individual who is usually quiet and reserved becomes vocal and angry about organization culture (*vocally unhappy actor* scenario); and where an individual who is usually vocal becomes withdrawn (*withdrawn actor scenario*). The other two scenarios presented the respondent with some form of evidence or an observable pattern which would be accompanied by a record, such as unusual working hours whereby access data could be used to evidence the activity (*unusual working hours scenario*) and negative remarks on social media (*social media bragging scenario)*. The 'Evidential Change' scenarios also included factors which may influence willingness to report. These were the relationship the observer has with the actor (long service and known, or new starter and unknown), and whether the actor is perceived to be more senior. The influence of employment status of the actor (contractor or permanent employee) and potential motivation of the actor (known work issues or personal issues) were also examined.

3.2 Procedure

A short structured questionnaire was developed, and piloted to test suitability and clarity of questions. Following the pilot some minor changes were made to wording and the final question was expanded to cover factors which may help facilitate reporting as well as factors that would prevent intervention. Once these changes were made, a list of managers by grade and department was obtained with assistance from the HR department, and this together with reference to organization charts was used to select the survey participants. Participants were informed that the survey was voluntary and confidential and ethical approval was obtained

from the University of Portsmouth for the research. The survey was emailed to a total of 102 recipients in July 2011, 55 of whom responded (14 Directors, 26 Managers and 11 staff graded employees). This is consistent with the average response rate for organizational surveys of this kind [59].

The survey included four scenarios designed to provide contexts that allowed exploration of reactions to potential behavioral precursors to the insider act and establish whether observers would report behavioral indicators of insider acts in the absence or presence of additional physical evidence (see Table A). For all scenarios the respondent was asked to consider which of the following actions they would take: report to the line manager, report to an anonymous helpline, talk to the person yourself or do nothing. The response 'talk to the person yourself' was included because some of the behaviors could be displayed as a result of somebody needing help or assistance, rather than being a security concern. Therefore this option allowed the respondent to indicate that they would have that conversation first, to help decide whether further intervention might be required.

The *unusual working hours* scenario included two additional options: to report to security or follow up with the individual the next day. For each scenario there was a free format text box titled 'other' allowing any other actions or comments to be recorded. After each scenario, the respondent was asked to consider whether any of a number of potential influencing factors would make them more or less likely to act or have no impact on their intention to act.

The influencing factors that were measured were divided into three main groups; relationship to the actor; employee status of the actor and potential motivations of the actor. The relationship to the actor (long service and known, versus being a new starter and not known) and the relative seniority of the actor to the observer were measured, as well as the influence of the employment status of the actor (whether the person was a contractor or permanent).

The potential motivations of the actor included work issues (such as performance management or grievances) as well as non-work related personal issues (significant life events such as bereavement, divorce, or debt for example) that might create a motive or vulnerability to the insider act.

The final question in the survey tested more general attitudes to reporting, and whether perceptions about how the report would be dealt with and the potential consequences would have an impact on decision to report or intervene. The factors that were measured were: confidence of confidentiality, quality of evidence, quality of process for reporting or intervention, fear of reprisal, not being sure how to handle the situation, and perceived relevance of motivation for behavioral changes. Respondents were asked to indicate whether each factor 'may encourage', 'may prevent' or have 'no impact' on reporting. A free format text field was also included for any other comments.

4.0 Results

4.1 Behavior change scenarios

Table B shows that the majority of participants would approach the actor in both the *withdrawn actor* scenario (88.5%) and the *vocally unhappy actor* scenario (61.2%), rather than reporting more formally through other mechanisms. However, twice as many would report the actor in the *vocally unhappy actor* scenario (16.3%) as would in the *withdrawn actor* scenario (7.7%). All respondents would take some kind of action in response to the *withdrawn actor* scenario, but four respondents (8.16%) would either 'wait and see' or 'do nothing' in response to the *vocally unhappy actor* scenario. In the *withdrawn actor* scenario, there were two comments which suggested that the respondent would talk to the individual first but that they might also raise it with the line manager; either in parallel, or if they were not comfortable with the answers they received from the actor. In the *vocally unhappy actor*

scenario, there were seven comments in the 'other' field, which also included multiple actions, such as talking to the person and also raising it with the line manager. One respondent thought that the person may be just be letting off steam, and a separate comment questioned why this scenario would indicate there was a problem, particularly if they agreed with the individual regarding issues with management and culture.

4.2 Evidential change scenarios

Table B shows a different pattern of responses for the evidential change scenarios, with a majority of participants in the *social media bragging* scenario (55.1%) and the *unusual working hours* scenario (63.27%) indicating that they would report the behavior either to the line manager, security or via a helpline. Approximately a third of respondents (32.7% in the *social media bragging scenario* and 30.6% in the *unusual working hours scenario*) would talk to or question the actor directly. The five respondents who intended to take other actions in relation to the *social media bragging* scenario indicated that they would talk to the individual and also discuss the situation with the line manager or contact the confidential helpline. The three respondents who identified an 'other' response to the *unusual working hours* scenario also indicated that there would be more than one route of discussion or escalation that they would take, such as seeking advice from their line manager or colleagues, reporting to security for example.

4.3 Factors influencing likelihood of intervention in each scenario

Table C shows that very few of the factors that were predicted to influence the decision to report or intervene were reported by participants as affecting their decision in these scenarios.

The majority of respondents indicated that their relationship to the actor would not have an impact on their intention to intervene irrespective of scenario type, although it was more

likely to influence intention than employee status. For example, in three of the four scenarios (*withdrawn actor, vocally unhappy actor* and *social media bragging* scenarios), approximately a third of respondents (32.7%, 34.7% and 36.7% respectively) indicated that they would be more likely to intervene if the actor was a long term employee who was well known to them. Interestingly, there was a very similar pattern of responses to new starters, with the majority indicating it would have no impact but a sizeable minority (32.7%, 25%, 32.7% and 40.8% across each scenario) suggesting it would make them more likely to intervene. There was only one scenario – *unusual working hours* – in which length of service was associated with less intention to act. The most influential relationship factor was seniority of the actor, with a majority of respondents (51.9%) indicating that they would be less likely to intervene with a senior actor in the *withdrawn actor* scenario and a substantial minority (40.8%) indicating it would make them less likely to intervene in the *unusual working hours* scenario.

Similarly, employment status of the actor had very little impact on intention to intervene, although it had more impact in the evidential change scenarios with 26.5% of respondents in the *social media bragging* scenario and 46.9% of respondents in the *unusual working hours* scenario indicating that they would be more likely to report if the actor was a contractor.

The impact of known work issues on likelihood of intervention was clearer for the evidential change scenarios (when it had either no impact or meant that respondents would be more likely to intervene) than it was for behavioral scenarios that produced a more mixed pattern of responses. For example, in the *withdrawn actor* scenario, 34.6% indicated that known work issues would make them more likely to intervene whereas 23.1% indicated it would make them less likely to intervene. Known personal issues also tended to have no impact or encourage respondents to intervene across three of the scenarios. However, for the *withdrawn actor* scenario, 32.7% indicated it would make them more inclined to intervene and 25%

indicated it would make them less likely to intervene, again demonstrating less consensus in response to this scenario.

4.4 Factors which may encourage or inhibit intervention in general (not specific to the scenarios)

Table D shows that the factors most likely to encourage intervention were ‘confidence of confidentiality’ (88.9%) and ‘having a clear process for reporting or intervention’ (84.6%). The factors most likely to act as a barrier to intervention were ’no hard evidence and may be mistaken’ (66.7%), ‘not sure how to handle the situation’ (61.1%), and ‘fear of reprisal’ (56.3%).

Additional comments received included re-emphasis that the seniority of the actor would be an inhibitor to intervention, as would feeling that there would be repercussions should they raise concerns. One respondent also commented that political correctness might inhibit reporting.

5.0 Discussion

The survey results supported existing research regarding the reluctance of employees to report changes in a colleague’s behavior in the context of scenarios where behavioral indicators of attitude change were not accompanied by more overt changes in behavior. However, our study shows that this does not reflect a tendency towards inaction, but rather an inclination to discuss the change directly with the actor in the first instance. Furthermore, in scenarios where some form of evidence was available, such as where a colleague overtly bragged about counterproductive workplace behaviors (CWBs) on social media or exhibited unusual working patterns, a majority of respondents would report the behavior. This demonstrates a willingness to report unambiguously suspicious behavior and supports our hypothesis that observers are more likely to report in scenarios where behavior change is

accompanied by evidence. This is further supported by the fact that a lack of evidence coupled with a concern that behavioral indicators may be mistaken was identified as the most common inhibitor of intervention in our study, suggesting that the provision of clear guidance regarding how to identify CWBs may increase reporting of behavioral indicators of insider threats in CNI organizations.

Although these results indicate that employees of CNI organizations may be more willing to take action in response to behavioral indicators than previous research would suggest, some respondents would wait, do nothing or delay their actions until the day after an observed event. This is important, as it introduces the risk that by the time questions are asked or actions taken that the insider act may already have taken place. Information for employees on how to respond to suspicious behavior therefore needs to include guidance on how to deal with situations of uncertainty in a timely manner, and organizations need to develop a positive security culture in which employees are confident to respectfully challenge unusual behaviors. A workplace environment in which CWBs are known to be challenged can also act as a deterrent to potential insider actors. The employee relationship factor that had the most inhibitory impact on willingness to intervene in the scenarios presented in our study was seniority. This supports our hypothesis that the relationship between the actor and the observer influences reporting likelihood, and is consistent with barriers and facilitators to intervention that were reported at a more general level, namely confidence of confidentiality and fear of reprisal. CNI organizations could address these barriers via the provision of processes for confidential reporting that circumnavigate line management chains of command.

The perceived motivations of the actor were also shown to have the potential to reduce willingness to intervene in scenarios where behavioral indicators of attitude change were not accompanied by behaviors or patterns which could be evidenced. It may be that in situations

of ambiguity, the attribution of personal or work-based motivations provides an alternative explanation for behavior to intention to commit an insider act, which supports our hypothesis that difficulties in interpreting the behavior could lead to non-intervention. The provision of information that demonstrates the links between these types of motivation and insider threat may therefore mitigate this barrier. However, further research is required to confirm this explanation.

When asked to consider factors that would more generally encourage or inhibit intervention, perceived organizational response, in particular confidence of confidentiality, and having a clear process for reporting and intervention were the most important facilitators for intervention. This supports our hypothesis that reporting routes should be made clear to employees. This also illustrates that CNI organizations need to recognize their own role in encouraging or deterring intervention and reporting. The primary barriers to intervention related to the employees' perception of their own ability to make an accurate judgements or knowing how to act. This supports our hypothesis that if the employee is uncertain about their competence this will inhibit reporting. These barriers can also be addressed at an organizational level by the provision of clear information about what constitutes suspicious behavior and regarding appropriate, proportionate responses for employees when observing CWBs.

6.0 Methodological Limitations

Our survey measured behavioral intentions rather than objectively measured behavior. Although behavioral intentions have been established as key determinants of behavior, there is also evidence to suggest that other factors including volitional control and social reaction are likely to affect whether actual behavior reflects intentions [60]. The fact that our findings regarding reluctance to act on behavioral indicators alone is consistent with previous research based on responses to genuine incidents [11, 12, 24, 26, 29, 32, 34, 37] provides some

reassurance on this issue. As with all surveys, the use of self-report data means that results may be subject to social desirability bias. However, the low levels of reporting behavior exhibited in the behavioral change scenarios suggests that social desirability effects have not had a strong influence on responses. The sample was limited in size and focused on only one organization within the energy sector; however the results do suggest that there are ways in which the insider act could be detected earlier through greater awareness of behaviors of concern. This provides an important opportunity for CNI organizations to prevent issues in the workplace from escalating and becoming a potential threat to the availability of critical services. The findings would need to be tested across different CNI organizations to confirm whether similar results would be obtained.

A final caveat is that despite the provision of a free text box to capture other comments and thoughts from participants, it was not possible to provide a conclusive explanation for unexpected responses. For example, why it is that when the relationship to the actor had an impact on an observer's intention to act it did not have a consistent effect for evidential change scenarios (i.e. it made respondents more likely to intervene in the *social media bragging* scenario, but made respondents both more and less likely to act in the *unusual working hours* scenario)? Furthermore, it is surprising that both knowing an actor well and being unfamiliar with the actor would influence likelihood of intervention in the same direction (i.e. increase the likelihood of intervention) for most scenarios. Further qualitative research is needed to explore the influence of these factors in more detail.

7.0 Conclusion

Employees may change during their employment and events within and outside of the workplace can lead to pressures which have the potential to lead to an insider act. Research has shown that a change in behavior, or mindset and attitude, is often displayed either prior to

or during the insider act being committed. These behaviors are usually evident to those who work with the individual, but often not mentioned or brought forward until the insider act has happened and is being investigated. Pre-employment screening is important, but cannot be the sole mitigating factor used by organizations against the insider threat; particularly in the context of CNI organizations because evidence of changed behavior or potential indicators associated with the insider act may only be observable when the person has been in post for a while. This study aimed to determine what types of behavior employees in a CNI organization would report and whether there were any influencing factors associated with the actor or the relationship with the actor that may encourage or inhibit reporting. The scenarios included evidential change and behavioral change in order to determine whether there would be different reporting appetites between the two.

The main findings from this study are that when presented with scenarios containing just behavioral issues or changes to normal behavior, participants were more likely to intervene by talking to the individual themselves than instigating formal reporting mechanisms. In contrast, if there was some form of evidence to accompany the behavior, participants were more likely to report to the line manager, to security or via an anonymous helpline. This suggests that the line manager may therefore be an important point of intervention and that CNI organizations should ensure that managers are equipped with the ability to know how to effectively handle a situation if brought to their attention.

The survey results indicate that people are often reluctant to report on the basis of observed behavior in case the situation has been misinterpreted, and as a result of concerns that there may be repercussions if they are incorrect. The link between changed behavior and a potential security issue may not always be apparent to CNI employees and this is an area which should be addressed by training and awareness. This highlights implications for CNI organizations in terms of the need for greater levels of awareness amongst employees about

the insider threat and specifically what indicators may be observable. It is also important to ensure that if behaviors are observed, employees know what they should do about it. Having a strong intervention and reporting system in place may help CNI organizations to encourage earlier intervention.

8.0 Acknowledgements

The data presented in this paper was originally collected as part of a National Grid funded MSc study that was conducted at the University of Portsmouth under the supervision of Dr Graham Brooks.

References

[1] W. Ashford, 2018 could be year of critical infrastructure attacks, says report, in: ComputerWeekly.com, https://www.computerweekly.com/news/450432690/2018-could-be-year-of-critical-infrastructure-attacks-says-report, 2018.
[2] NCSC, NCSC deals with 1,100 cyber attacks in first two years, in, https://www.ncsc.gov.uk/news/ncsc-deals-1100-cyber-attacks-first-two-years, 2018.
[3] S. Williamson, Countering the Threat of Physical Security Breaches, The Data Centre Journal, (2017).
[4] CPNI, Threats, in, https://www.cpni.gov.uk/threats-0, 2018.
[5] E.D. Shaw, K.G. Ruby, J.M. Post, The Insider Threat to Information Systems: The Psychology of the Dangerous Insider, Security Awareness Bulletin, 21 (1998) 1 - 10.
[6] E.E. Schultz, A framework for understanding and predicting insider attacks, Computers & Security, 21 (2002) 526-531.
[7] F.L. Greitzer, R.E. Hohimer, Modeling Human Behavior to Anticipate Insider Attacks, Journal of Strategic Security, 4 (2011) 25-48.
[8] M. Bunn, S.D. Sagan, A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes, American Academy of Arts and Sciences, Cambridge, Mass., 2014.
[9] C. Alcaraz, S. Zeadally, Critical infrastructure protection: Requirements and challenges for the 21st century, International Journal of Critical Infrastructure Protection, 8 (2015) 53-66.
[10] ACFE, Report to the Nations on Occupational Fraud and Abuse, in, http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf, 2014.
[11] T. Noonan, E. Archuleta, The National Infrastructure Advisory Council's Final Report and Recommendations on The Insider Threat to Critical Infrastructure, in, The National Infrastructure Advisory Council, https://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf, 2008, pp. 1 - 55.
[12] F.L. Greitzer, L.J. Kangas, C.F. Noonan, A.C. Dalton, R.E. Hohimer, Identifying At-Risk Employees: Modeling Psychosocial Precursors of Potential Insider Threats, in: 2012 45th Hawaii International Conference on System Sciences, 2012, pp. 2392-2401.
[13] S. Swann, Rajib Karim: The terrorist inside British Airways, in: BBC, 2011.
[14] BBC, Lloyds bank worker Jessica Harper jailed for £2.4m fraud, in: BBC, http://www.bbc.co.uk/news/uk-england-london-19675834, 2012.
[15] S. Gaudin, Ex-UBS Systems Admin Sentenced To 97 Months In Jail, in, Information Week, 2006.
[16] BBC, Profile: Waheed Mahmood, in: BBC, 2007.
[17] D.A. Mundie, S. Perl, C.L. Huth, Toward an Ontology for Insider Threat Research: Varieties of Insider Threat Definitions, in: 2013 Third Workshop on Socio-Technical Aspects in Security and Trust, 2013, pp. 26-36.
[18] M. Hanley, T. Dean, W. Schroeder, M. Matt Houy, R.F. Trzeciak, J. Montelibano, An Analysis of Technical Observations in Insider Theft of Intellectual Property Cases, in, Software Engineering Institute, Carnegie Mellon University, 2011, pp. 35.
[19] S.L. Pfleeger, J.B. Predd, J. Hunker, C. Bulford, Insiders Behaving Badly: Addressing Bad Actors and Their Actions, Information Forensics and Security, IEEE Transactions on, 5 (2010) 169-179.
[20] P.G. Neumann, The challenges of insider misuse, in: Workshop on Preventing, Detecting, and Responding to Malicious Insider Abuse, Aug. 16-18, 1999, SRI Computer Science Laboratory, Santa Monica, 1999.
[21] D.M. Cappelli, A.P. Moore, R.F. Trzeciak, The CERT Guide to Insider Threats, Pearson Education, Inc., United States of America, 2012.
[22] A.P. Moore, D.M. Cappelli, R.F. Trzeciak, The big picture" of insider IT sabotage across U.S. critical infrastructures, in, CMU-CERT, Software Engineering Institute, Carnegie Mellon University website: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8703, 2008.

[23] S.R. Band, D.M. Cappelli, L.F. Fischer, A.P. Moore, E.D. Shaw, R.F. Trzeciak, Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis, in, Carnegie Mellon Software Engineering Institute, USA, 2006, pp. 1 - 108.
[24] CPNI, Insider Data Collection Study, Report of Main Findings, in, https://www.cpni.gov.uk/Documents/Publications/2013/2013003-insider_data_collection_study.pdf, 2013.
[25] Director of Central Intelligence / Intelligence Community Staff Memorandum, Project Slammer Interim Progress Report, in, http://www.foia.cia.gov/sites/default/files/document_conversions/89801/DOC_0000218679.pdf, 1990.
[26] A. Jones, C. Colwill, Dealing with the Malicious Insider, in: Proceedings of the 6th Australian Information Security Management Conference, Edith Cowan University, Edith Cowan University Research Online, Perth, Western Australia, 2008.
[27] V. Gisladottir, A.A. Ganin, J.M. Keisler, J. Kepner, I. Linkov, Resilience of Cyber Systems with Over- and Underregulation, Risk Analysis, 37 (2017) 1644-1651.
[28] P.-J.K. Linkov I., Trump B.D., Ganin A.A., Kepner J., Rulemaking for Insider Threat Mitigation, in: L.I. Kott A. (Ed.) Cyber Resilience of Systems and Networks. Risk, Systems and Decisions, Springer, Amsterdam, 2019
[29] A.P. Moore, D.M. Cappelli, T.C. Caron, E. Shaw, D. Spooner, R.F. Trzeciak, A Preliminary Model of Insider Theft of Intellectual Property, in, Carnegie Mellon, Software Engineering Institute, Carnegie Mellon University website: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9855, 2011.
[30] P.A. Legg, N. N. Moffat, J.R.C. Nurse, J. Happa, I. Agrafiotis, M. Goldsmith, S. Creese, Towards a Conceptual Model and Reasoning Structure for Insider Threat Detection, (2014).
[31] A. Cummings, T. Lewellen, D. McIntire, A.P. Moore, R. Trzeciak, Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector, in, Software Engineering Institute, Carnegie Mellon, 2012.
[32] K.L. Herbig, Changes in Espionage by Americans: 1947-2007, in, Defense Personnel Security Research Center, 2008.
[33] P.J. Taylor, C.J. Dando, T.C. Ormerod, L.J. Ball, M.C. Jenkins, A. Sandham, T. Menacere, Detecting insider threats through language change, Law and Human Behavior, 37 (2013) 267-275.
[34] M. Keeney, E. Kowalski, D. Cappelli, A. Moore, T. Shimeall, S. Rogers, Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors, in, U.S Secret Service and CERT Coordination Center/SEI, https://resources.sei.cmu.edu/asset_files/SpecialReport/2005_003_001_51946.pdf, 2005, pp. 45.
[35] M.R. Randazzo, M. Keeney, E. Kowalski, D. Cappelli, A. Moore, Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector, in, U.S. Secret Service and CERT® Coordination Center/SEI, 2005, pp. 25.
[36] C. Colwill, Human factors in information security: The insider threat – Who can you trust these days?, Information Security Technical Report, 14 (2009) 186-196.
[37] S. Wood, J.C. Marshall-Mies, Improving Supervisor and Coworker Reporting of Information of Security Concern, in, Defense Personnel Security Research Center (PERSEREC), http://www.dhra.mil/perserec/reports/tr02-03.pdf, 2003.
[38] S. Clough, Ten years in jail for BAE worker who tried to sell secrets, in: The Telegraph, https://www.telegraph.co.uk/news/uknews/1426680/Ten-years-in-jail-for-BAE-worker-who-tried-to-sell-secrets.html, 2003.
[39] C. McGreal, Hacker turns in US soldier over WikiLeaks Iraq video, in: The Guardian, http://www.theguardian.com/world/2010/jun/07/hacker-wikileaks-iraq-video-manning, 2010.
[40] PERSEREC, COUNTERINTELLIGENCE REPORTING ESSENTIALS (CORE) A Practical Guide for Reporting Counterintelligence and Security Indicators, in: D.P.S.R.C. (PERSEREC) (Ed.), http://www.dhra.mil/perserec/reports/core_brochure.pdf, 2004.
[41] P.R. Sackett, The Structure of Counterproductive Work Behaviors: Dimensionality and Relationships with Facets of Job Performance, International Journal of Selection and Assessment, 10 (2002) 5-11.

[42] W.S. Albrecht, G.W. Wernz, T.L. Williams, Fraud : bringing light to the dark side of business, Irwin Professional Pub, Burr Ridge, Ill, 1995.
[43] B. Latané, J.M. Darley, The unresponsive bystander : why doesn't he help?, Appleton-Century-Crofts, New York, 1970.
[44] T. Moriarty, Crime, Commitment, and the Responsive Bystander: Two Field Experiments, Journal of Personality and Social Psychology 197S, 31 (1975) 370-376.
[45] D.R. Shaffer, M. Rogle, C. Hendrlck, Intervention in the Library: The Effect of Increased Responsibility on Bystanders' Willingness To Prevent a Theft, Journal of Applied Social Psychology, 5 (1975) 303-319.
[46] L. Schwarz, K. Jennings, J. Petrillo, R. Kidd, Role of commitments in the decision to stop a theft., The Journal of Social Psychology, 110 (1980) 183–192.
[47] N. Guéguen, M. Dupré, P. Georget, C. Sénémeaud, Commitment, crime, and the responsive bystander: effect of the commitment form and conformism, Psychology, Crime & Law, 21 (2015) 1-8.
[48] B. Latane, D. Elman, The hand in the till, in: B. Latané, J.M. Darley (Eds.) The unresponsive bystander: Why doesn't he help?, Appleton-Century-Crofts, New York, 1970.
[49] L. Bowes-Sperry, A.M. O'Leary-Kelly, To Act or Not to Act: The Dilemma Faced by Sexual Harassment Observers, The Academy of Management Review, 30 (2005) 288-306.
[50] A.M. Ryan, J.L. Wessel, Sexual orientation harassment in the workplace: When do observers intervene?, Journal of Organizational Behavior, 33 (2012) 510-511.
[51] C. Baez-Leon, B. Moreno-Jimenez, A. Aguirre-Camacho, R. Olmos, Factors influencing intention to help and helping behaviour in witnesses of bullying in nursing settings, Nurs Inq, 23 (2016) 358-367.
[52] P. Desrumaux, T. Machado, G. Vallery, L. Michel, Bullying of the Manager and Employees' Prosocial or Antisocial Behaviors: Impacts on Equity, Responsibility Judgments, and Witnesses' Help-Giving, Negotiation and Conflict Management Research, 9 (2016) 44-59.
[53] M.J. Williams, J.G. Horgan, W.P. Evans, The critical role of friends in networks for countering violent extremism: toward a theory of vicarious help-seeking, Behavioral Sciences of Terrorism and Political Aggression, 8 (2016) 45-65.
[54] R. Searle, C. Rice, Assessing and Mitigating the Impact of Organisational Change on Counterproductive Workplace Behaviour: An Operational (Dis)trust Based Framework, in, Centre for Research and Evidence on Security Threats, 2018, pp. 100.
[55] B. Latané, J. Rodin, A lady in distress: Inhibiting effects of friends and strangers on bystander intervention, Journal of Experimental Social Psychology, 5 (1969) 189-202.
[56] J.M. Darley, B. Latane, Bystander intervention in emergencies: diffusion of responsibility, J Pers Soc Psychol, 8 (1968) 377-383.
[57] S. Ghumman, A.M. Ryan, J.S. Park, Religious harassment in the workplace: An examination of observer intervention, Journal of Organizational Behavior, 37 (2016) 279-306.
[58] P. Fischer, J.I. Krueger, T. Greitemeyer, C. Vogrincic, A. Kastenmuller, D. Frey, M. Heene, M. Wicher, M. Kainbacher, The bystander-effect: a meta-analytic review on bystander intervention in dangerous and non-dangerous emergencies, Psychol Bull, 137 (2011) 517-537.
[59] Y. Baruch, Response Rate in Academic Studies-A Comparative Analysis, Human Relations, 52 (1999) 421-438.
[60] T.L. Webb, P. Sheeran, Does changing behavioral intentions engender behavior change? A meta-analysis of the experimental evidence, Psychological Bulletin, 132 (2006) 249-268.

Table A: Scenario descriptions

Behavior change scenarios	
Withdrawn actor	'A usually lively, team player has become increasingly withdrawn, does not want to engage in conversation, and has become more likely to react angrily to requests for deadlines to be met'.
Vocally unhappy actor	'A team member who has always been quiet and respectful, has recently become very vocal about how, in their opinion, the company does not adhere to the values it expects from its employees'.
Evidential change scenarios	
Social media bragging	'An employee who holds a specialist post has been bragging to others on the team about the damage they could do to the company if they so chose. You are friends with the person outside of work, communicating occasionally on social networking sites. You have noticed that the person has been posting similar boasts alongside negative remarks about the company, on a publicly accessible website'.
Unusual working hours	'As part of your role, you are required to work irregular hours and occasional weekends. You have noticed that an employee from a department which does not normally operate unusual working patterns has frequently been in the office late at night and at weekends on their own. One evening in particular you saw them access the building with someone who didn't appear to have their own ID card'

Table B: Frequencies (percentages) for intended actions following observation of change in behavior only (behavoral scenarios) and changed behavior accompanied by form of evidence (evidential scenarios)

	Wait	Report to line manager	Report to helpline	Report to Security*	Talk to the person / contact them the following day	Approach person and ask what they are doing*	Other	Nothing
Behavioral change:								
Withdrawn actor	0 (0)	4 (7.7)	0 (0)	N/A	**46 (88.5)**	N/A	2 (3.8)	0 (0)
Vocally unhappy actor	3 (6.1)	8 (16.3)	0 (0)	N/A	**30 (61.2)**	N/A	7 (14.3)	1 (2)
Evidential change:								
Social media bragging	0 (0)	15 (30.6)	12 (24.5)	N/A	**16 (32.7)**	N/A	5 (10.2)	1 (2)
Unusual working hours	0 (0)	13 (26.5)	1 (2)	**17 (34.7)**	4 (8.2)	11 (22.4)	3 (6.1)	0 (0)

***These response options were only used in the *Unusual Working Hours* scenario**

Table C: Frequencies (percentages of people who responded) for whether factors influenced likelihood of intervention in each scenario

	Behavior change scenarios				**Evidential change scenarios**			
	Withdrawn actor		Vocally unhappy actor		Social media bragging		Unusual working hours	
Relationship to the actor: impact on likelihood of intervention								
Long service, known actor	More	17 (32.7)	More	17 (34.7)	More	18 (36.7)	More	9 (18.4)
	Less	0 (0)	Less	2 (4.1)	Less	0 (0)	Less	13 (26.5)
	No impact	**35 (67.3)**	No impact	**30 (61.2)**	No impact	**31 (63.3)**	No impact	**27 (55.1)**
New starter, unknown actor	More	17 (32.7)	More	12 (25)	More	16 (32.7)	More	20 (40.8)
	Less	4 (7.7)	Less	0 (0)	Less	0 (0)	Less	0 (0)
	No impact	**31 (59.6)**	No impact	**36 (75)**	No impact	**33 (67.3)**	No impact	**29 (59.2)**
Seniority	More	1 (1.9)	More	4 (8.3)	More	8 (16.3)	More	4 (8.2)
	Less	**27 (51.9)**	Less	12 (25)	Less	11 (22.4)	Less	20 (40.8)
	No impact	25 (48.1)	No impact	**32 (66.7)**	No impact	**30 (61.2)**	No impact	**25 (51)**
Employment status of the actor: impact on likelihood of intervention								
Permanent	More	7 (13.5)	More	5 (10.4)	More	5 (10.2)	More	5 (10.4)
	Less	0 (0)	Less	0 (0)	Less	1 (2)	Less	1 (2.1)
	No impact	**45 (86.5)**	No impact	**43 (89.6)**	No impact	**43 (87.8)**	No impact	**42 (87.5)**
Contractor	More	5 (9.6)	More	7 (14.6)	More	13 (26.5)	More	23 (46.9)
	Less	7 (13.5)	Less	1 (2.1)	Less	2 (4.1)	Less	0 (0)
	No impact	**40 (76.9)**	No impact	**40 (83.3)**	No impact	**34 (69.4)**	No impact	**26 (53.1)**
Potential motivations of the actor: impact on likelihood of intervention								
Work issues	More	18 (34.6)	More	13 (27.1)	More	20 (40.8)	More	19 (38.8)
	Less	12 (23.1)	Less	8 (16.7)	Less	0 (0)	Less	0 (0)
	No impact	**23 (44.2)**	No impact	**27 (56.3)**	No impact	**29 (59.2)**	No impact	**30 (61.2)**
Personal issues	More	17 (32.7)	More	8 (16.7)	More	13 (26.5)	More	10 (20.4)
	Less	13 (25)	Less	4 (8.3)	Less	2 (4.1)	Less	2 (4.1)
	No impact	**22 (42.3)**	No impact	**36 (75)**	No impact	**34 (69.4)**	No impact	**37 (75.5)**

Table D: Frequencies (percentages) of factors that would encourage or inhibit willingness to intervene in general

	May encourage	May prevent	No impact
Perceived organizational response			
Confidence of confidentiality	**32 (88.9)**	0 (0)	4 (11.1)
Clear process for reporting / intervention	**33 (84.6)**	0 (0)	6 (15.4)
Fear of reprisal	1 (3.1)	**18 (56.3%)**	13 (40.6)
Perceived competency (own)			
No hard evidence, and may be mistaken	2 (5.6)	**24 (66.7%)**	10 (27.8)
Not sure how to handle the situation	2 (5.6)	**22 (61.1%)**	12 (33.3)
Perceived motivation (actors)			
May be issues outside of work	3 (7.9)	8 (21.1%)	**27 (71.1)**